SPECIFICATION AMENDMENTS

Please replace the paragraph beginning on page 4, line 7 with the following replacement paragraph:

To address the need in the art for a DRM system that meets both consumers and content providers expectations, U.S. ~~Serial~~ Patent Application No. 09/542,510, entitled "Digital Rights Management Within an Embedded Storage Device," filed April 3, 2000, now U.S. Patent No. 6,636,966, U.S. ~~Serial~~ Patent Application No. 09/583,452, entitled "Method of Decrypting Data Stored on a Storage Device Using an Embedded Encryption/Decryption Means," filed May 31, 2000, U.S. ~~Serial~~ Patent Application No. 09/940,026, entitled "Host Certification Method and System," filed August 27, 2001, U.S. ~~Serial~~ Patent Application No. 09/940,083, entitled "A Secure Access Method and System," filed August 27, 2001, now U.S. Patent No. 7,110,982, describe a DRM system in which the DRM "intelligence" has been integrated into the storage engine. As opposed to conventional DRM systems that reside on the host, the integrated storage engine approach is far less vulnerable to hacking by a user of a host system – the user has no access to the DRM functionality within the storage engine other than through the reading or writing of secure content from the storage medium associated with the storage engine. The user knows that digital content may flow to and from the data storage medium but cannot access the "how" within the storage engine that enabled such movement. Moreover, the integration of the DRM system into the storage engine is advantageous in portable applications. Different host systems such as kiosks at a content provider retail outlet or a personal computer may be more readily modified to couple to the portable DRM-system-integrated storage engine.

performs an additional encryption on this encrypted content using a Data Encryption Standard (DES) algorithm in encryption block 415. This encryption may occur using single, double, or triple DES encryption as described in U.S. Patent Application ~~Serial~~ No. 09/583,452, entitled "Method of Decrypting Data Stored on a Storage Device Using an Embedded Encryption/Decryption Means," filed May 30, 2000, the contents of which are hereby incorporated by reference. The corresponding DES key or keys are generated in DES key generation module 425. Using secure session key 60, data storage engine decrypts the AES key in AES key decryption block 420. The AES key is then DES-encrypted and the DES key(s) and the encrypted AES key are then stored in secure area 40 of disc 25. The associated doubly-encrypted data content is stored in file system area 85 of disc 25.

LC 3/03/09

Please replace the paragraph beginning on page ~~16~~ 28, line ~~22~~ 7 with the following replacement paragraph:

In the embodiments described above, the storage engine 20 is relatively "dumb" in that it has no ownership of the file system used to with respect to the encrypted content on disc 25. For example, although storage engine 20 may have file-system-object-level access to security metadata in embodiments incorporating a security repository, storage engine 20 has no knowledge regarding the physical blocks a given file system object may occupy on disc 25. This knowledge is retained by host system 5, which must perform the translation of a file system object request into the corresponding block level request. In contrast to such an approach, U.S. Patent ~~Serial~~ Application No. 09/539,841, entitled "File System Management Embedded in a Storage Device," filed March 31, 2000, now